

Claims

- 5 1. An item, attached to a product which is subjected to a chain of logistics, for
collection of data and for communication with a host computer via a data
network, the item comprises an electronic module including a unique identity
identifying each item individually and a non-retrievable cryptographic key and the
host computer is storing the corresponding identity and cryptographic key,
10 **characterized by** that the electronic module stores collected data related to the
product or use of the product in a non-volatile memory and a cryptographic
operation is performed on the collected data when exchanged between the item
and the host computer in order to ensure identity, authenticity, integrity and
confidentiality of the collected data.
- 15 2. An item, in accordance with claim 1, **characterized by** that sensors are applied
to the product in a way that the electronic module can receive, store and process
data generated by the sensors.
- 20 3. An item in accordance with claim 1 or 2, **characterized by** that the electronic
module comprises a time-keeping means for generating a time-stamp to be
stored together with pre-stored data and the collected data.
- 25 4. An item in accordance with claim 1, 2, or 3, **characterized by** that the non-
volatile memory holds an address to the host computer for allowing automatic
connection to the host computer via the data network.
- 30 5. An item in accordance with claim 1, 2, 3, or 4, **characterized by** that the
cryptographic key can be supported by a cryptographic processor to perform
encryption or decryption using a symmetric algorithm.
6. An item in accordance with claim 1, 2, 3, 4 or 5, **characterized by** that the
cryptographic key can be supported by a cryptographic processor to perform
encryption or decryption using an asymmetric algorithm.

- 5 7. An item in accordance with claim 5 or 6, **characterized by** that an additional independent cryptographic key issued by a third party, is stored in the electronic module, the additional key being used to perform at least one cryptographic operation on stored data, in order to enable the third party to use a result of the cryptographic operation to ensure integrity of the stored data.
- 10 8. An item in accordance with any of the preceding claims, **characterized by** that the sensors comprise printed conductive traces connected to the electronic module.
- 15 9. An item in accordance with claim 8, **characterized by** that the printed conductive traces are applied in a pattern as to enable detection of disposal of an individually packed element from the product.
- 20 10. An item in accordance with claim 9, **characterized by** that the printed conductive traces are applied in a pattern as to enable detection of attempts to remove the item attached to the product.
- 25 11. An item in accordance with any of the preceding claims, **characterized by** that the sensors comprise measurement means for measuring a property like temperature, humidity or chemical elements.
- 30 12. A product, being a part of a logistic chain and having sensors for measuring a property, **characterized by** that the product has an item in accordance with one or more of the preceding claims attached to it.
13. A method for gathering data generated by a multitude of products being part of a logistic chain and each product having an item attached to it, the item comprising an electronic module for communicating with a host computer via a data network and said electronic module comprising a unique identity and a non-retrievable cryptographic key, **characterized by** that
- the generated data is collected and stored by a memory means of the electronic module;

- the cryptographic key performs an encryption operation on the generated data;
- the generated data is transmitted together with the unique identity to the host computer via a data network;
- the host computer is decrypting the transmitted data with a cryptographic key stored in the host computer together with the unique identity given to the item.

5

14. A method according to claim 13, **characterized by** that the memory means processes the stored collected data before it is decrypted and transmitted to the host computer.

10

15. A method according to claim 13 or 14, **characterized by** that the item is provided with data characterizing the product or a user of the product before the product to which the item is attached is sent to a first station of its logistic chain.

15

16. A method according to claim 13, 14 or 15, **characterized by** that the electronic module receives encrypted data from the host computer when the product is at a station of its logistic chain and the received data is decrypted by the stored cryptographic key and stored in the memory means.

20

17. A method according to claim 13, 14, 15 or 16, **characterized by** that the electronic module comprises a time keeping means which generates a time stamp each time new data is received by the memory means.

25

18. A method according to one or more of claims 13-17, **characterized by** that a third party generates an additional cryptographic key which is stored in a separate data-base and in the electronic module of the item and the additional cryptographic key is used by an auditor to verify the gathered collected data at the host computer.

30